Serial No.: 09/705,998

IN THE SPECIFICATION:

Please amend the SPECIFICATION as follows:

On page 48 replace the abstract with the following paragraph:

The present invention provides encryption schemes and apparatus which securely generate a cipher-text which in itself contains checks for assuring message integrity. It also provides compatible decryption schemes ~~and apparatus to decrypt the cipher-text~~ confirming message integrity. The encryption scheme generates a cipher-text with message integrity in a single pass with little additional computational cost, while retaining at least the same level of security as schemes based on a MAC. One embodiment encrypts a plain-text message by dividing the plain-text message into a multitude of plain-text blocks and encrypting the plain-text blocks to form a multitude of cipher-text blocks. A single pass technique is used in this process to embed a message integrity check in the cipher-text block. ~~Embodiments are described to decrypt the cipher-text blocks to reform the plain-text blocks, and perform message integrity check in the cipher-text blocks.~~ A message integrity check is embedded in the cipher-text blocks by embedding a ~~generating a random number and a~~ set of pseudo random numbers, which may be dependent, but are pair-wise differentially uniform. We also describe an embodiment which is highly parallelizable. ~~Although a pair-wise differentially uniform sequence is a weaker property than the pair-wise independent sequence, it is shown that it can be computationally cheaper to generate. The random numbers are used to embed the message integrity check in the cipher text blocks. During the decryption process, the random numbers are obtained from the cipher-text blocks, and as the cipher-text blocks are decrypted, the pseudo random numbers are used to reform the plain-text blocks from the cipher-text blocks.~~